RECEIVED
CENTRAL FAX CENTER

NOV 0 3 2005

DOCKET NO. SC11015ZC

Launched by Motorola
freescale semiconductor

FAX TRANSMITTAL SHEET

Freescale Semiconductor, Inc.
Law Department
7700 W. Parmer Lane
MD: TX32/PL02
Austin, TX 78729
Telephone: (512) 996-6839
Facsimile: (512) 996-6854

14 Number of Pages (including this page)

Date: November 3, 2005

To: Matthew T. Henning – 2131

Location: United States Patent and Trademark Office

Fax No.: (571) 273-8300

From: James L. Clingan, Jr. - 30,163

Subject: 09/725,821– James D. Dworkin et al

MESSAGE:

Enclosed herewith, please find an APPEAL BRIEF for filing in the below-identified application.

ALL ITEMS MARKED WITH AN "X" ARE INCLUDED:

1.	x	1 page Facsimile Cover Sheet
2.	x	11 page Appeal Brief
3.	X	1 page Fee Transmittal (in duplicate)

Paid by Deposit Account: 503079 $500

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING FACSIMILE TRANSMITTED TO THE PATENT AND TRADEMARK OFFICE.

ON: 11/3/05 (Date) _____ (Signature)

PLEASE GIVE THESE PAPERS TO:

EXAMINER: Matthew T. Henning
GROUP ART UNIT: 2131
SERIAL NO.: 09/725,821
FILED: NOVEMBER 29, 2000
Inventor: James D. Dworkin et al

RECEIVED
OIPE/IAP

NOV 0 4 2005

FEE TRANSMITTAL

Patent fees are subject to annual revision

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500

Complete if Known	
Application Number	09/725,821
Filing Date	November 29, 2000
First Named Inventor	James D. Dworkin et al
Examiner Name	Matthew T. Henning
Group Art Unit	2131
Attorney Docket No.	SC11015ZC

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 503079

Deposit Account Name: FREESCALE SEMICONDUCTOR, INC.

The Director is authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) during the pendency of this application

☐ Charge fees(s) indicated below, except for the filing fee to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)		Fee Paid
1001	790	2001	395	Utility filing fee	
1002	300	2002	175	Design filing fee	
1003	550	2003	275	Plant filing fee	
1004	790	2004	395	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES

			Previously Paid**		Extra Claims		Fee from below		Fee Paid
Total Claims		-	20	=		X	50	=	
Independent Claims		-	3	=		X	200	=	
Multiple Dependent							300	=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Code
1202	50	2202	9	1202
1201	200	2201	44	1201
1203	300	2203	150	1203
1204	88	2204	44	1204
1205	18	2205	9	1205

SUBTOTAL (2) ($)

** or number previously paid, if greater; For Reissues, see above.

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	
1051	130	2051	65	Surcharge – late filing fee or oath	
1052	50	2052	25	Surcharge – late Provisional filing	
1053	130	1053	130	Non-English specification	
1812	2520	1812	2520	For filing a request for ex parte Reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1840*	1805	1840*	Requesting publication of SIR after Examiner action	
1251	120	2251	55	Extension for reply within first month	
1252	450	2252	215	Extension for reply within second month	
1253	1020	2253	490	Extension for reply within third month	
1254	1590	2254	765	Extension for reply within fourth month	
1255	2160	2255	1040	Extension for reply within fifth month	
1401	500	2401	170	Notice of Appeal	
1402	500	2402	170	Filing a brief in support of an appeal	500
1403	1000	2403	150	Request for oral hearing	
1451	1510	1451	1510	Petition to institute a public use proceeding	
1452	500	2452	55	Petition to revive – unavoidable	
1453	1500	2453	685	Petition to revive – unintentional	
1501	1400	2501	685	Utility issue fee (or reissue)	
1502	490	2502	245	Design issue fee	
1503	660	2503	330	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of IDS	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	
Large Fee	790	2801	395	Request for Continued Examination	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify)

SUBTOTAL (3) ($) 500

* Reduced by Basic Filing Fee Paid

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	James L. Clingan, Jr.	Registration No.	30,163	Telephone	(512) 996-6839
Signature	James L. Clingan, Jr.	Date	NOV 7, 2005		

RECEIVED
CENTRAL FAX CENTER
NOV 03 2005

In re Application of:
James D. Dworkin, et al.
Serial No.: 09/725,821
Filed: November 29, 2002
For: A CIRCUIT FOR GENERATING HASH VALUES

November 3, 2005

Art Unit: 2131
Examiner: Matthew T. Henning
Docket No.: SC11015ZP

Certificate of Transmission under 37 CFR 1.8

I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office.

on November 3, 2005

Signature

Stacie Herrera
Printed Name of Person Signing Certificate

REPLY BRIEF

COMMISSIONER FOR PATENTS
ALEXANDRIA, VA 22313
BOARD OF PATENT APPEALS & INTERFERENCES:

This reply brief is filed in the matter of the Appeal to the Board of Appeals and Interferences of the rejection of the claims of the above-referenced application for patent.

11/04/2005 HDEMESS1 00000019 503079 09725821
01 FC:1402 500.00 DA

STATUS OF CLAIMS

Claims 1-8 and 14-18 are pending. Claims 9-13 have been canceled.

Claims 1-7, 14, 15, 17, and 18 stand rejected under 35 U.S.C. 103(a) as being obvious in view of Ober et al., U.S. Patent No. 6,708,273 (Ober); Childs, U.S. Patent No. 5,623,545 (Childs); Bruce Schneier, Applied Cryptography (Schneier); Turner et al., U.S. Patent No. 4,896,296 (Turner); and Batcher, U.S. Patent No. 4,314,349 (Batcher). Claim 8 stands rejected under 35 U.S.C. 103 (a) as being obvious in view of Ober, Childs, Schneier, Turner, Batcher and Niehaus et al., U.S. Patent No. 4,399,517 (Niehaus). Claim 16 stands rejected under 35 U.S.C. 103 as being obvious in view of Ober, Childs, Schneier, Turner, Batcher, and Masaki, U.S. Patent No. 4,739,195 (Masaki).

The rejection of claims 1-8 and 14-18 is being appealed.

GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL

1) Are claims 1-7, 14, 15, and 18 obvious under 35 U.S.C. 103(a) in view of Ober et al., U.S. Patent No. 6,708,273 (Ober); Childs, U.S. Patent No. 5,623,545 (Childs); Bruce Schneier, Applied Cryptography (Schneier); Turner et al., U.S. Patent No. 4,896,296 (Turner); and Batcher, U.S. Patent No. 4,314,349 (Batcher)? Is claim 8 obvious under 35 U.S.C. 103 (a) in view of Ober, Childs, Schneier, Turner, Batcher and Niehaus et al., U.S. Patent No. 4,399,517 (Niehaus)?

2) Is claim 16 obvious under 35 U.S.C. 103 in view of Ober, Childs, Schneier, Turner, Batcher, and Masaki, U.S. Patent No. 4,739,195 (Masaki)?

3) Is dependent claim 17 obvious under 35 U.S.C. 103 in view of Ober, Childs, Schneier, Turner, and Batcher.

ARGUMENT

The Examiner raised new points of argument in Grounds 1 and 3 to which applicants respond as follows:

GROUND 1

The Examiner pointed out that not all of the elements of FIG. 1 of applicants application are present in claim 1. Applicants point out, however, that it appears that the Examiner would consider FIG. 1 obvious based on his view of what one of ordinary skill in the art would do with the references used by the Examiner in rejecting claim 1 and dependent claims 2-7. Applicant's believe it is instructive to look at the references taken together and comparing them to applicants' FIG. 1.

GROUND 3

The Examiner argued that the applicants did not actually claim in claim 17, which depends on claim 15, that the register arrays were shared for both the SHA-1 and MD5 functions. Perhaps that is technically true but even assuming arguendo that it is true it is a distinction without a meaningful difference. The register array, as claimed, has one claimed characterisitic for one function (claim 15) and a different characteristic for the other function (claim 17). The Examiner pointed out that Ober has a single register array. The Examiner did not, apparently because it was not possible to do so, argue that the register array of Ober met either of the characteristics as claimed. Accordingly, applicants do not see much merit to this position except to say that registers can be used for a lot of different things. The Examiner then argued that the register array of Childs provides both claimed characteristics. Even if true, this is insufficient because Childs performs only one of the claimed functions. Thus claim 15 and claim 17 cannot both be met by the register array of Childs. Accordingly, applicants submit that there is not a sufficient showing in the prior art for the notion of the register array providing both claimed characteristics and also being operational during both functions.

CONCLUSION

For at least the reasons set forth above and in the appeal brief, Applicants respectfully submit that the claims of the present application are allowable over the art cited during prosecution.

Respectfully submitted,

James L. Clingan, Jr.
Attorney for Appellants
Reg. No. 30,163
Ph: (512) 996-6821

Claims Appendix

1. An apparatus for selectively processing first and second cryptographic hash algorithms, comprising:

a register file (12) having at least five registers for storing chaining variables;

a function circuit (22) receiving first (B), second (C) and third (D) chaining variables and an output that provides a logical data value;

a first multiplexer (24) having an input coupled to the register file for receiving a fourth (E) chaining variable and an output that provides the fourth chaining variable when the first cryptographic hash algorithm is being processed by the apparatus and a zero value when the second cryptographic hash algorithm is being processed by the apparatus; and

a summing circuit (30) having a first input coupled to the output of the function circuit for receiving the logical data value, a second input coupled to the output of the first multiplexer, and an output coupled to the register file.

2. The apparatus of claim 1, further comprising:

a barrel shifter (40) having an input coupled to the output of the summing circuit;

an adder (41) having an input coupled to an output of the barrel shifter; and

a second multiplexer (42) having a first input coupled to the output of the summing circuit and a second input coupled to an output of the adder.

3. The apparatus of claim 2, further comprising:

a third multiplexer (26) having a first input coupled to the output of the second multiplexer (42) and a second input coupled to the register file (12) for receiving a fifth (A) chaining variable; and

a fourth multiplexer (28) having a first input coupled to the output of the second multiplexer and a second input coupled to the register file (12) for receiving the third (D) chaining variable.

4. The apparatus of claim 3, wherein the second multiplexer and the fourth multiplexer receive a signal that transfers a summed value from the output of the summing

circuit to the register file when the message digest hardware accelerator is processing an SHA-1 hash algorithm.

5. The apparatus of claim 3, wherein the second multiplexer and the third multiplexer receive a signal that transfers a summed value from the output of the barrel shifter to the register file when the message digest hardware accelerator is processing an MD5 hash algorithm.

6. The apparatus of claim 3, further comprising:

a first shift circuit (16) having an input coupled to the register file for receiving the first (B) chaining variable; and

a fifth multiplexer (14) having a first input coupled to an output of the first shift circuit, a second input coupled to the input of the first shift circuit and an output coupled to the register file for providing the second chaining variable.

7. The apparatus of claim 6, further comprising:

a second shift circuit (18) having an input coupled to the register file for receiving the fifth (A) chaining variable; and

a sixth multiplexer (20) having a first input coupled to an output of the second shift circuit, a second input coupled to the input of the second shift circuit and an output coupled to another input of the summing circuit.

8. A circuit for generating hash values in a first hash mode and a second hash mode, comprising:

a storage circuit (34, 36);

a register array (32) having registers for storing a message and an output for providing a round dependent data value (Wt);

a register file (12) for storing first (B), second (C), third (D), fourth (E) and fifth (A) chaining variables; and

an adder (30) having a first input coupled for receiving a first set of constant values stored in the storage circuit for the first hash mode and a second set of constant values for

the second hash mode, a second input coupled to the output of the register array, a third input coupled for receiving the fifth (A) chaining variable in the second hash mode and a shifted fifth chaining variable in the first hash mode, a fourth input coupled for receiving a logical function in accordance with the first, second and third chaining variables, and a fifth input coupled for receiving the fourth chaining variable in the second hash mode and a zero value in the first hash mode.

14. An apparatus integrated to provide a hash value of a variable length message in accordance with a first algorithm and a second algorithm, comprising:

a register file (12) having five registers preset to a first group of values for the first algorithm and to a second group of values for the second algorithm, the register file storing first (B), second (C), third (D), fourth (E) and fifth (A) chaining variables;

a function circuit (22) receiving first, second and third chaining variables and generating a first logical data value for the first algorithm and a second logical data value for the second algorithm;

a storage element (34, 36) for supplying a first set of constant values for the first algorithm and a second set of constant values for the second algorithm; and

a summing circuit (30) having a first input coupled to the output of the function circuit (22) and a second input coupled to the storage element for receiving one of the first and second sets of constant values.

15. The apparatus of claim 14, further including a register array (32) having a decoder circuit (120) and a plurality of registers for selecting a data word stored in one of the plurality of registers and supplying the data word to an output of the register array when computing the first algorithm.

16. The apparatus of claim 15, wherein the register array further includes:

an exclusive-OR (116) coupled for simultaneously receiving first, second, third and fourth data words stored in the plurality of registers; and

a rotate block (118) having an input coupled to an output of the exclusive-OR and supplying a one bit left circular shift of the data generated by the exclusive-OR to one of the registers in the plurality of registers.

17. The apparatus of claim 15, wherein an output of the register array is supplied from a word wise circular queue when computing the second algorithm.

18. The apparatus of claim 14, wherein the first algorithm is an MD5 algorithm and the second algorithm is an SHA-1 algorithm.

Evidence Appendix

No evidence is submitted in this appendix

Related proceedings Appendix

There are no decisions under this appendix.